National Infrastructure Protection Center
NIPC Daily Open Source Report
for 31 January 2003

Current Nationwide Threat Level is

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports a new study, in a Princeton journal, warns that a successful terrorist attack on a spent fuel storage pool at a large nuclear reactor could have very serious consequences, and it goes on to make recommendations on safety measures. (See item 2)
- The Boston Globe reports that despite spending millions over the past 16 months to shore up airline security, a utility knife with a retractable blade was found on a United Air Lines jet, on Wednesday. (See item 13)
- Reuters reports the International Maritime Bureau warns that acts of piracy are rising sharply and global shipping is increasingly prone to terrorist attack −− especially attacks by militant groups like al Qaeda on tankers and merchant ships using small boats packed with explosives. (See item 17)
- PC Magazine reports gaps in national criminal laws are leaving doors open for cybercriminals, and many of the most insidious viruses and network attacks have emerged from places where no laws restrict such activities. (See item 33)
- The BBC News reports researchers at the San Diego Supercomputer Center, looking at problems that leave the Net open to attack, have analyzed web traffic on one root server and found that it spent most of its time dealing with unnecessary queries. (See item 34)
- Editors Note: The NIPC Daily Report is now available in PDF and Word on the NIPC website at http://www.nipc.gov/dailyreports/dailyindex.htm
- Editors Note: The Distribution of the NIPC Daily Report will be changing servers in preparation for the move to the Department of Homeland Security. The new mail host will be mail.nipc.osis.gov. The transition will happen starting Monday Morning February 3rd.

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 30, Pioneer Press* — **State's nuclear plants vulnerable.** Xcel Energy's two Minnesota nuclear power plants have taken added precautions since the terrorist attacks of September 2001, but key areas of the facilities remain vulnerable to a resourceful attacker, a state Senate committee was told Tuesday. **And while the generating plants at Prairie Island and Monticello have emergency notification systems to warn nearby residents if there's an accident, those procedures might be too slow in the event of an attack, David Lochbaum, a nuclear expert with the Union of Concerned Scientists, testified before the Senate's commerce and utilities committee. "No plants were designed with a 9/11−type thing in mind," Lochbaum said. "There are some vulnerabilities to the plants to that type of threat."** But when the committee's chairwoman, Sen. Ellen Anderson, DFL−St. Paul, asked Lochbaum what might be a "worst−case scenario" if a plant was hit by terrorists, a couple of the panel's members warned her not to bring up the subject. As it was, Lochbaum said the type of damage would depend on the type of attack. **The vulnerability of the country's 104 nuclear power plants has long been an issue, but it has taken on added significance since the 2001 attacks in New York and Washington, D.C. A special study group of the U.S. Nuclear Regulatory Commission said in an October 2000 report that there was a 50 percent chance of "catastrophic" damage if a large plane were flown into the building housing the spent fuel pool at a plant like Monticello.** After the 9/11 attacks, the report was removed from the NRC's Web site. Monticello and Prairie Island generate more than a third of the electricity produced by Northern States Power−Minnesota, the Xcel subsidiary that supplies power to 1.3 million customers in the state.
Source: http://www.twincities.com/mld/twincities/news/politics/50611 78.htm

2. *January 30, New York Times* — **Study warns attack on fuel could pose serious hazards. A successful terrorist attack on a spent fuel storage pool at a large nuclear reactor could have consequences "significantly worse than Chernobyl," according to a new scientific study. But it said the risk could be cut sharply by moving some of the spent fuel to dry casks near the reactors and making changes in how the rest is stored.** The paper will appear in the spring issue of Science and Global Security, a journal at Princeton. Some of its eight authors began briefing federal officials in Washington today. Their recommendations include reinforcing the casks to make them less vulnerable and designing them so that if a large airplane were crashed into them, the plane's fuel could not pool around them and overheat them as it burned. **The report is one of the few broad analyses of the risk posed by spent fuel that is being made public. Because there is no long−term storage site for nuclear fuel, the risk it poses would persist for years even if the reactors where it is now stored are shut down, as some critics are seeking for the Indian Point plants in New York.** Many reactor operators have already moved some fuel to dry casks because their pools have filled up as the federal program to bury the fuel has slipped further into the future. Burial can be done only with fuel that is more than five years old, because newer fuel gives off so much heat that it must be kept in water. The older fuel can be kept dry because air will safely dissipate its heat. It would cost

$3.5 billion to $7 billion to move old fuel to dry casks, the authors predicted. When the nuclear plants were designed, engineers believed that the fuel would be removed quickly from the pools, and were more concerned about releases from inside the containment, where water and steam at high temperatures and pressures seemed more prone to escape. **Spent fuel pools are designed to withstand earthquakes, hurricanes, tornadoes and other natural hazards, but were not explicitly designed with terrorism in mind.**
Source: http://www.nytimes.com/2003/01/30/national/30NUKE.html?tntem ail1

3. *January 30, Reuters* — **Indonesia takes steps to protect U.S. facilities. Indonesia's chief security minister, Susilo Bambang Yudhoyono, said Thursday Jakarta is acting to protect vital facilities such as those of major U.S. oil and mining firms in the event of war between the United States and Iraq.** Indonesia is the world's most populous Muslim country and opposition to a U.S. attack on Iraq is widespread, with many analysts predicting such an act could spark violence by extreme elements in the country. "We have to anticipate whatever happens outside Indonesia (to ensure) it should not rattle the domestic situation," Susilo Bambang Yudhoyono told reporters after meeting President Megawati Sukarnoputri. **"Our obligation is to anticipate and to implement proactive and preventive steps including for domestic vital facilities," he said when asked what the government would do to protect the Indonesian operations of oil companies ExxonMobil and Caltex Pacific Indonesia and copper and gold miner Freeport−McMoRan in the event of a U.S.−Iraq conflict.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A64686−2003Jan 30.html

4. *January 30, New York Times* — **Hartford official says planning is faulty at Indian Point plant. The Connecticut attorney general, Richard Blumenthal, has joined a chorus of New York voices charging that emergency plans are inadequate to provide for a huge evacuation in the event of a disaster at the Indian Point nuclear plant in Westchester County. In a letter sent Tuesday to Gov. George E. Pataki of New York, Blumenthal said that hundreds of thousands of Connecticut residents could be endangered by inadequate emergency planning, and he urged Pataki to support a temporary closing of Indian Point "in the interest of public safety."** This month, a report sponsored by New York State concluded that emergency planning was insufficient to protect residents from an extensive radiation release at Indian Point, either as a result of an accident or a terrorist attack. Current emergency plans cover only a 10−mile radius surrounding the plant. Most criticism of disaster planning at Indian Point has been focused in Westchester or Albany. But Blumenthal said Connecticut had to be involved. Four counties in New York have refused to certify the evacuation plan required by federal officials to keep the plant open. Governor Pataki is supposed to decide by Friday whether to certify the same plan. In his letter, Blumenthal urged Pataki not to do so. "In the event of a nuclear emergency, people will choose to evacuate an area far greater than 10 miles from Indian Point, possibly including a significant portion of Connecticut," Blumenthal wrote. "There is no assurance that they will be able to do so safely or effectively." **"The map is pretty startling," Blumenthal said in an interview today. "If you look at the major cities affected ˜ Danbury, Waterbury, Bridgeport, Stamford, the entire Fairfield County corridor ˜ it's one of the most densely populated and economically vital parts of the state, containing probably more than a third of the population." He said New York should also consider the limits of regional roadways. "I−95 already is a parking lot at certain times of day," he said.**
Source: http://www.nytimes.com/2003/01/30/nyregion/30INDI.html

5. *January 29, The Atlanta Journal−Constitution* — **Georgia clean−fuel rule likely to meet with delay.** Several big oil and gas companies say they can produce it, but the cleanest−burning gas probably won't be available in Atlanta until January of next year. **A state Board of Natural Resources committee on Tuesday agreed to relax a clean−fuel rule and give companies more time to phase in low−sulfur gasoline. The full board is expected to approve the change today. State environmental regulators recommended the change, bowing to pressure from oil suppliers and gas retailers who warned of gas shortages, price spikes and long lines at the pump.** Some oil companies wanted regulators to stick to the rule, a critical piece of the state's plan to clean up metro Atlanta's air. BP, Chevron and Shell said they are ready to meet the state's original requirement to sell fuel with only one−tenth the sulfur found in most gasoline by May 1. The fuel, which would be the cleanest in the country, would reduce noxious fumes and clear away some of the haze that settles over the skyline every summer. But without incentives, those companies said they won't bring the low−sulfur fuel to metro Atlanta because market economics make it too costly. They say they are already at a competitive disadvantage after spending millions of dollars on equipment to meet the state's original requirement. Most other major oil and gas suppliers, including Marathon Ashland Petroleum, and retailers they sell to such as QuikTrip, said they could not bring enough low−sulfur fuel to the metro Atlanta market in time. Rather than meet metro Atlanta's requirements, they are gearing up for a three−year phase−in of national clean−fuel requirements that begins next year. Those companies warned of gas shortfalls as high as 30 percent if the low−sulfur rule goes into effect. **When Georgia adopted the rule as part of a phase−in of clean gas in 1998, metro Atlanta was supposed to meet a Clean Air Act deadline this year. The deadline has since been postponed until next year. The original requirement for fuel that contains no more than 30 parts per million of sulfur would be pushed back to Jan. 1, 2004 −−− still earlier than the national phase−in.**
Source: http://www.energycentral.com/sections/gasnews/gn_article.cfm ?id=3604750

6. *January 29, Platts Global Energy News* — **LNG spot market seen developing to contain ship costs. A potential liquid natural gas (LNG) spot market is developing, driven by efforts to contain transportation costs, energy company officials said Wednesday at the Third Annual LNG: Economics and Technology Conference. More than 150 LNG vessels will be operating by 2004, 40 new ships are on order, and the size of ships is growing to more than 138,000 cu m. BG Group's BG LNG Services, now the biggest importer of LNG into the US, imports only spot market LNG, said the company's Vice President Howard Candelet.** "Transportation is the Achilles' Heel of the industry," said Candelet. "Any time you see an opportunity to ship LNG to one place and divert it to another place (where the price is higher), that's the way to go." The industry term for the practice is arbitrage, and accounts for 20% of BG's LNG trades, he said. LNG shippers can hedge by using forward spot prices, and LNG is competitive with gas, which is not normally sold on long−term contracts, Candelet said. However, each LNG trade, though done initially by phone with a counter party, requires a detailed legal contract, he said. **Increased security for all vessels calling into U.S. ports can cause delays, which can translate into costly shipment delays and going to the spot market to ensure on−time delivery, he added.** Companies should share shipping information, Candelet added. "At the moment, ships are crossing the Atlantic from Trinidad going to Europe full, and returning empty. And they are coming across the Atlantic in the other direction," he said. "The only way the industry will be right is to share information on shipping.

Source: http://www.platts.com/stories/gas2.html

[Return to top]

Chemical Sector

7. *January 30, Associated Press* — **Officials interview North Carolina plant workers.** Investigators sought the help of eyewitnesses Thursday for clues to the cause of an explosion and raging fire at a plastics factory that killed three people and injured 37 others. Ten people remained in critical condition, and officials said Thursday that another was unaccounted for. The explosion in a 40−foot−tall section of the West Pharmaceutical Services plant Wednesday sent flames and debris shooting into the air, touching off fires in the surrounding woods and shaking homes for miles. About 130 people were in the plant at the time. **The cause of the explosion was a mystery because the plant kept relatively little volatile material on site, West chief executive officer Don Morel said Thursday. The company, based in Lionville, Pa., near Philadelphia, makes pharmaceutical delivery and medical devices. Plant worker Wayne Brown said Thursday that only a few people work in the ``automatic compounding system'' section of the factory, where the explosion happened. There, mixing machines on an upper level create molten rubber, which is poured down to the ground level and cut into sheets as it cools, he said.** Plant workers began coming in Thursday morning to be interviewed by investigators from the U.S. Chemical Safety Board−−a federal investigative agency similar to the National Transportation Safety Board−−and other state and federal agencies. Plant maintenance worker Kevin Morgan said he was about 50 yards away from where the blast happened. He says he heard a single explosion, as loud as a jet engine. Morgan said the ceiling started caving in, the power went out and everything was dark. Someone nearby had a flashlight and everyone who was in there started evacuating to the parking lot. **The Occupational Safety and Health Administration (OSHA) said the plant was inspected in October, cited for numerous safety violations and fined about $10,000, an amount reduced to about $9,000 early this month. Since 1993, OSHA has inspected 443 similar facilities and found an average of nearly six violations per site, compared with 15 violations at West Pharmaceutical. Morel said there's no indication the violations−−including problems with its electrical systems design, wiring and portable fire extinguishers−−played any role in the explosion.**
Source: http://www.news−journal.com/news/content/news/ap_story.html/National/AP.V8907.AP−Factory−Explosi.html

[Return to top]

Defense Industrial Base Sector

8. *January 30, New York Times* — **Airlines and Pentagon discuss using commercial transport fleet.** The nation's airlines have held initial discussions with the Pentagon about mobilizing a fleet of commercial and air cargo planes for use in the event of a war with Iraq, aviation officials said yesterday. **Such an action would mark only the second time in history that the military had mobilized the Civilian Reserve Air Fleet, a standby arrangement that lets the Pentagon call upon up to 925 aircraft and their crews during global conflicts. The fleet,**

established in 1951, was used during the Persian Gulf war to transport troops and equipment abroad. The talks took place last week, said officials of the Air Mobility Command, based at Scott Air Force Base in Illinois. Maj. Gen. Roger A. Brady, director of operations for the command, spoke with officials of several of the two dozen airline and cargo carriers that take part in the air fleet, military officials said. **The primary purpose of the conversations, they said, was to ask carriers about their willingness to provide more charter planes for troop movements, short of a mobilization. No date for a mobilization has been set, aviation officials said.** Air carriers sign contracts pledging to take part in the fleet during military conflicts in return for Pentagon business during normal times. **A war in Iraq would be likely to result in the most limited mobilization, which would involve 78 passenger and cargo jets and up to 2,000 crew members, military and airline officials said.** Source: http://www.nytimes.com/2003/01/30/international/middleeast/3 0AIR.html

9. *January 30, Aviation Daily* — **NORTHCOM Official: don't shift money from combat air patrols.** U.S. Northern Command faces a number of challenges, but money earmarked for combat air patrols over the next several years shouldn't be diverted to help solve the challenges, according to Lt. Gen. Edward G. Anderson III, NORTHCOM's deputy commander. "My feeling is no, I don't think it would" be right to shift the amount, apparently $700 million, away from the CAPs, Anderson said in response to a question at a conference here. **"I think the CAPs serve a multitude of purposes," he said. "First and foremost ... they serve as a deterrent against any kind of" aerial activity by terrorists. The CAPs have been in place since the Sept. 11, 2001 terrorist attacks using hijacked airliners. "I don't think we should ignore the fact that there are potential threats that could come from the air," Anderson said. "We have responsibility for air and maritime [threats], and ... the only way you're going to stop them is if you've got something airborne, that's for sure." In addition, Anderson said at SpaceComm 2003, sponsored by the Armed Forces Communications and Electronics Association, "I think the American public ... gets a sense of security from [the CAPs] and recognizes that there is a presence there from Northern Command and NORAD [North American Aerospace Defense Command] to be able to provide that level of support."** He declined to say whether $700 million was too much. "I'm not going to comment on that," he said. "I'll leave that to the budgeteers."
Source: http://ebird.dtic.mil/Jan2003/s20030130150321.html

10. *January 30, Inside the Pentagon* — **Senators want National Guard role in homeland security defined.** Sen. Diane Feinstein (D−CA), backed by the co−chairs of the Senate National Guard Caucus, introduced a bill Jan. 23 to encourage states to develop plans on how they would deploy the National Guard for homeland security purposes. **Congressional sources say homeland security is at the top of the legislative agenda, as Congress works to approve an omnibus appropriations bill for fiscal year 2003. Eleven FY−03 appropriations bills were left uncompleted at the close of last year; the FY−03 defense appropriations bill was passed in December.** Feinstein first offered her legislation last year as an amendment to the FY−03 defense authorization bill, but it was not included in the version signed by President Bush, according to a spokesman for the senator. This year's proposal has been referred to the Senate Armed Services committee, after garnering support from Senate National Guard Caucus co−chairmen Christopher Bond (R−MO) and Patrick Leahy (D−VT). The bill has not been scheduled for mark−up, Feinstein's spokesman said. **Her bill would allow the defense secretary to provide funds to state governors who need to activate the Guard to perform**

homeland security activities. Governors first would need to submit a plan stating how they intend to use the Guard. For instance, the Guard could assist the Department of Homeland Security's directorate of immigration affairs "in the transportation of aliens who have violated a federal or state law prohibiting terrorist acts," the bill states. The "Guard Act of 2003" is modeled after the existing National Guard counterdrug program, and tracks the recommendations of several blue−ribbon antiterrorism commissions, including the October 2002 Council on Foreign Relations−sponsored Hart−Rudman task force report and the congressionally chartered Hart−Rudman and Gilmore commissions.
Source: http://ebird.dtic.mil/Jan2003/s20030130150255.html

[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

11. *January 31, CNN On Line* — **Tanker falls from overpass, explodes.** A truck hauling propane gas plunged from a freeway overpass and exploded in a huge fireball early Thursday, killing the driver and cutting a power line that serves 1,100 people. The tanker was headed west on Interstate 69 shortly after midnight when it struck a set of guardrails dividing an off−ramp from the main road. The truck skidded, rolled on its side over the overpass railing, and dropped 35 feet onto railroad tracks below. The truck caught fire and burned for several minutes before exploding with a fireball that shot flames 600 feet into the air, witnesses said.
Source: http://www.cnn.com/2003/US/Midwest/01/30/tanker.explosion.ap /index.html

12. *January 30, Washington Post* — **Agency plans to ease pilots into gun−training program. The federal government's plan to allow commercial airline pilots to carry guns will begin cautiously, with just 50 pilots in the initial program,** the Transportation Security Administration said Wednesday. The TSA, which was directed by Congress last year to develop a training program by Feb. 25 for pilots to carry guns, has yet to finalize decisions about other details of the program, such as the exact date training will begin, how guns will be transported to airplanes and how pilots will interact with federal air marshals. **The agency plans spend $500,000 for an initial program that is scheduled to start in the next several months. The test phase with the 50 pilots will last several weeks before the agency launches a full−scale program**, said Robert Johnson, a TSA spokesman. Tens of thousands of pilots are expected to eventually participate. "It's prudent to test the curriculum on a smaller group than to begin a full−scale implementation right from the beginning," Johnson said. **Pilots will be trained at Federal Law Enforcement Training Centers in Glynco, Ga., and Artesia, N.M., where federal agents such as those from the Federal Bureau of Investigation, U.S. Customs Service, Federal Air Marshal Service and the U.S. Border Patrol also train.** Pilots who undergo the training will be called "federal flight deck officers" and **must complete recurrent training.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A63517−2003Jan 29.html

13. *January 30, Boston Globe* — **Logan security gap exposed by find.** Despite spending millions over the past 16 months to shore up airline security, the complex organization overseeing the new system was scrambling Wednesday to answer basic questions raised by Tuesday's scare at Logan Airport, where a sharp tool was found on a United Air Lines jet. **Twenty−four hours after the security breach, officials could not say how the tool got on the plane or offer assurances that such incidents will not happen again.** Federal security officials and the airline could not even agree on what exactly was found on San Francisco−bound Flight 179, and provided contrasting interpretations of the severity of the incident. **The breach − whether accidental or intentional − highlighted a major gap in the nation's airline security involving the lack of searches of workers who maintain and service aircraft.** Brian Doyle, spokesman for the federal Transportation Security Administration, said **background checks on workers are done by airports and airlines, but the TSA has no policy to have airline employees, including maintenance workers, screened or searched by security.** United officials in Illinois said Wednesday that the tool found was an awl that is used to align holes in sheet metal. But George Naccara, Logan's federal security director for the Transportation Security Administration, closely examined the object at a morning security meeting and said it was a utility knife with a retractable blade.
Source: http://www.boston.com/dailyglobe2/030/metro/Logan_security_gap_exposed_by_find+.shtml

14. *January 30, Transportation Security Administration* — **Southwest Florida International Airport to require boarding passes at the security checkpoint starting Thursday.** Under Secretary of Transportation for Security Adm. James M. Loy announced on Thursday that **Southwest Florida International Airport (RSW), Ft. Myers, FL, is joining more than 140 other airports today in participating in the Transportation Security Administration's "Selectee Checkpoint" program.** The program enhances security and convenience by transferring the screening of selectees from aircraft boarding gates to security checkpoints where screening equipment and personnel and law enforcement officers are concentrated. At Southwest Florida International Airport, passengers must now have their boarding passes in hand before they reach the security checkpoint. E−ticket receipts, itineraries and vouchers will no longer provide access through the checkpoints, and boarding passes will no longer be issued at the gates. Boarding passes may be obtained at ticket counters, through airline computer kiosks, or at most skycap curbside stations. In addition to a boarding pass, passengers must show a valid government issued photo ID, such as a driver's license or passport at the checkpoint. In keeping with TSA's multi−level security system at all airports, TSA screeners will now choose gates, flights and passengers at random for additional screening at the gates.
Source: http://www.dot.gov/affairs/tsa0903.htm

15. *January 30, Federal Computer Week* — **TSA to award system to check travelers. The Transportation Security Administration plans to award a contract next month to a systems integrator for a tool that will perform background checks and risk assessments on airline travelers.** The contractor also will provide the risk assessment engine for the Computer Assisted Passenger Pre−Screening II program. **CAPPS II, a substantially advanced version of the system now in use, is being designed to cull multiple government and commercial databases for information that could indicate a potential threat. The intent is to "improve the ability to identify threats to aviation security by analyzing and evaluating**

multiple−source data on every ticketed passenger on every airline to determine whether the passenger poses a security risk or threat to the traveling public," TSA officials wrote in a presolicitation notice posted on FedBizOpps.gov. **"The approach creates a configurable threat assessment tool that allows real−time adjustment of threat priorities."** The current system makes threat information available to airline employees, who are then supposed to pass it on to airport security staff. CAPPS II will distribute alerts directly to front−line forces in near−real time, according to a report officials wrote about the tool.
Source: http://www.fcw.com/fcw/articles/2003/0127/web−tsa−01−30−03.a sp

16. *January 30, General Accounting Office* — **Major management challenges and program risks: Department of Transportation.** On Thursday, the General Accounting Office (GAO) issued a performance and accountability report on the Department of Transportation (DOT). In its report, GAO found that DOT has implemented a number of actions to improve its mission and management performance. Future improvements will increasingly demand effective partnerships and consensus−building with state, local, and private stakeholders. After conducting its review of DOT, the GAO concluded that the department should work with Congress and other transportation stakeholders to develop approaches that **improve transportation safety, mobility through intermodal and modal planning and investment approaches,** and human capital strategies; **pursue strategies to address long−term security challenges and ensure a smooth transition to Department of Homeland Security responsibility;** and continue to improve its acquisition and financial management by addressing root causes of problems.
Source: http://www.gao.gov/pas/2003/d03108.pdf

[Return to top]

Postal and Shipping Sector

17. *January 30, Reuters* — **Global ship piracy up again, terrorism feared.** Acts of piracy are rising sharply and global shipping is increasingly prone to "terrorist" attack, an ocean crime watchdog said on Thursday. **In its 2002 annual report the International Maritime Bureau (IMB), which monitors crime on the high seas, said the attacks on shipping worldwide rose steeply to 370 incidents last year compared to 335 in 2001. The IMB highlighted the dangers of a new and disturbing trend: attacks by militant groups like al Qaeda on tankers and merchant ships using small boats packed with explosives.** In direct reference to the attack on the French tanker the Limburg, rammed by an explosive−laden boat in the Gulf of Aden last October, it said such acts would be difficult to stop. "The risk of terrorist attack can perhaps never be eliminated, but sensible steps can be taken to reduce the risk," the IMB said in a statement. **It recommended that port authorities designate approach channels under coast guard or police supervision from which all other craft would be banned. The IMB said most attacks were on ships at anchor.** The IMB's sternest warning was saved for **the waters around Somalia which it ranked as the "most dangerous" in the world. "The risk of attack...from Somali armed militias has now increased from one of possibility to certainty,"** it said. **The IMB also reported a disturbing steep rise in hijackings up from 16 to 25 incidents.** Many, it said, were committed in the now notorious Malacca Straits and waters off Indonesia.
Source: http://www.washingtonpost.com/wp−dyn/articles/A64768−2003Jan 30.html

[Return to top]

Agriculture Sector

18. *January 30, Reuters* — **Mad cow disease still a risk. The World Health Organization warned on Thursday that many countries, particularly in eastern Europe and southeast Asia, were at risk from mad cow disease, even though the worst appeared over in Britain.** Although most developed countries had adequate measures in place to fight the deadly infection in cattle, which has been linked to more than 100 human deaths, some other states had not woken up to the dangers, it said. **"Our concern is that there are countries out there which may be developing bovine spongiform encephalopathy (BSE) and are not doing anything about it," said Dr. Maura Ricketts, of WHO's animal and food−related public health risks division.** The WHO official, presenting a report on the BSE threat, said contaminated meat and bone meal animal feed were known to have been exported to a number of countries where few or no cases of the fatal disease had yet been reported. Far from being a cause for concern, the reporting of cases could be a reassuring sign the authorities were taking steps to detect infection and to eradicate the problem, she said. **"Central and eastern European countries as a whole were large importers of this material. Slovakia, Slovenia and the Czech Republic have reported cases but other countries need to be checking this," she added. Southeast Asia, along with parts of North Africa, were other areas where significant amounts of contaminated feed had been imported from Western Europe, she said.**
Source: http://www.alertnet.org/thenews/newsdesk/L30408037

19. *January 30, Clarion−Ledger* — **Poultry industry faces virus threat. The poultry industry in Leake and Neshoba counties, in Mississippi, have stepped up precautions to stem the spread of laryngotracheitis, a highly contagious disease, which can kill infected birds.** The disease, which poses no danger to humans, strikes poultry during winter months, and was diagnosed in the area about Jan. 8, said Billy Mack Stuart, vice president of First Financial Bank in Carthage, which specializes in poultry lending. One of the poultry companies advised area growers by letter on Jan. 9, he said. Mississippi state Veterinarian Dr. Jim Watson said there were "a few cases of that and we're doing some vaccinating up there as a precaution against the spreading of the disease." **The virus was detected through routine testing of poultry at the state diagnostic laboratory, Dr. Watson said. From there, growers and processors were told to take precautions.** Carthage grower Kirby Nazary is one of two growers who have suffered losses because of the virus. Nazary said the precautions in place are thorough and should wipe out the virus. Some growing areas restrict all but state officials and veterinarians hired by the companies to check the health of birds, he said. "What I'm hearing from the state officials is this is a vaccine−induced strain. And what we're hearing is the naturally occurring strain is worse," Nazary said. "Whoever vaccinated the pullets didn't do it just right. It's a live virus, but it's very contagious.
Source: http://www.clarionledger.com/news/0301/30/b01.html

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

20. *January 30, Water Tech Online* — **Water security assessments will have secure submission guidelines, EPA says. The U.S. Environmental Protection Agency (EPA) is providing a set of instructions to assist water utilities in submitting self−assessments to the agency in a secure fashion.** G. Tracy Mehan III, EPA's assistant administrator for water, said in a news release that drinking water utilities are already submitting vulnerability assessments to EPA, which marks a significant milestone in the efforts to protect drinking water supplies. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires EPA to work with water utilities to protect vital infrastructure and public health. **Under the Bioterrorism Act, all community drinking water systems that serve more than 3,300 people are required to certify and submit vulnerability assessments and certify completion of emergency response plans to EPA.**
Source: http://www.watertechonline.com/news.asp?mode=4font>

[Return to top]

Public Health Sector

21. *January 30, USA Today* — **Officials promote BioShield.** Giving the government unprecedented authority to buy and distribute vaccines and antidotes against bioterrorism would hasten the development of new and better drugs, administration officials said Wednesday. **In his State of the Union address Tuesday, President Bush proposed Project BioShield, which would provide about $6 billion over 10 years to combat smallpox, anthrax and botulinum toxin, a deadly food poisoning agent. "We must assume that our enemies would use these diseases as weapons, and we must act before the dangers are upon us," he said.** The need for bioterrorism drugs and vaccines is great. Botulinum toxin, for instance, is one of Saddam Hussein's major bioweapons. Yet the source of the nation's best antidote could dry up this year: California's antitoxin program faces elimination as a result of the state's record $35 billion deficit. **Under the plan, the government could guarantee drug companies a buyer for their products. Without that guarantee, pharmaceutical companies have been reluctant to spend what it takes to develop and produce the needed medicines, officials said. "Fundamentally, this is a program that is geared toward accelerating the process of research, development, purchase and availability to the public of things to counter bioterrror attacks," said Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases at the National Institutes of Health.** Food and Drug Administration Commissioner Mark McClellan said the $6 billion figure was arrived at based on "a careful analysis of the threats against this country."
Source: http://www.usatoday.com/news/washington/2003−01−29−biosheild −usat_x.htm

22. *January 30, Associated Press* — **CDC chief: bioterror threat remains real. More than a year has passed since anthrax attacks kept the nation on edge, and the chief of the U.S. Centers for Disease Control and Prevention (CDC) worries that people have forgotten.**

"Many people have put that issue in the back of their mind. We've relaxed," Dr. Julie Gerberding, director of the CDC, said in an interview Wednesday with The Associated Press. **"Complacency is the enemy of preparedness. And we really have to keep reminding people: They're still out there."** Dr. Gerberding, who took over the CDC last summer, has spent much of her tenure developing and now putting in place a smallpox vaccination program aimed at preparing the nation should the virus return in a bioterror attack. In the first phase of the vaccination program, the CDC had hoped to vaccinate as many as 450,000 people on smallpox response teams and in hospital emergency rooms. Dr. Gerberding sought to lower expectations, saying she will not be disappointed if the final number of people vaccinated in the first phase does not reach 450,000. **The ultimate question, she said, is, "Are you prepared?" "That's what we will be monitoring," she said. So far, CDC officials said, 38 states, plus Los Angeles County and Cook County, IL, which includes Chicago, have requested 205,700 doses of vaccine for their programs, and 127,200 doses have been delivered to 22 states and those two counties.** One state, Connecticut, began inoculations last week; several others are expected to begin this week. In the end, the total is not likely to reach 450,000 people and could be significantly lower, an administration official said Wednesday.
Source: http://www.washingtonpost.com/wp−dyn/articles/A64616−2003Jan 30.html

23. *January 30, Stars and Stripes* — **Two show significant adverse effects to smallpox vaccine. Two military members recently showed "significant adverse effects" to the smallpox vaccine, though the symptoms are not life−threatening, defense officials said.** One of the two patients began showing the adverse signs over the weekend and the other on Tuesday, Army Lt. Col. John Grabenstein, deputy director for military vaccines, said Wednesday during a health conference. **Since President Bush ordered on Dec. 13 a mandatory smallpox vaccination program that eventually will tap roughly 500,000 troops, about three percent of those vaccinated have lost one or more days at work or reported side effects such as fever or malaise, Grabenstein said.** There have been no reported deaths. To date, roughly 3,000 military health−care workers have gotten the vaccine. The number in the operational force is not releasable to the public, he said. However, both the Center for Disease Control and Prevention and the Food and Drug Administration are updated weekly on the number and health status of vaccinated troops.
Source: http://www.stripes.osd.mil/article.asp?section=1042784

[Return to top]

Government Sector

24. *January 30, General Accounting Office* — **Protecting information systems supporting the federal government and the nation's critical infrastructure.** On Thursday, the General Accounting Office (GAO) released a report in its High−Risk Series on protecting information systems that support the federal government and the nation's critical infrastructure. In its report, the GAO writes that since January 2001, efforts to improve federal information security have accelerated at individual agencies and at the governmentwide level. For example, implementation of Government Information Security Reform legislation (GISRA) enacted by the Congress in October 2000 was a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. **In implementing GISRA, agencies have noted benefits, including increased management**

attention to and accountability for information security. Although improvements are under way, recent audits of 24 of the largest federal agencies continue to identify significant information security weaknesses that put critical federal operations and assets in each of these agencies at risk. Over the years, various working groups have been formed, special reports written, federal policies issued, and organizations created to address the nation's critical infrastructure challenges. In 1998, the President issued Presidential Decision Directive 63 (PDD 63), which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber−based systems essential to the minimum operations of the economy and the government. To accomplish its goals, PDD 63 designated and established organizations to provide central coordination and support. This directive has since been supplemented by Executive Order 13231, which established the president's Critical Infrastructure Protection Board and the President's National Strategy for Homeland Security. While the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, GAO has made numerous recommendations over the last several years concerning CIP challenges. In response to these challenges, improvements have been made and efforts are in progress, but more work is needed to address them. **Among other actions essential to sustaining federal information security improvements are the agencies' development of effective risk management programs and the development of a comprehensive strategy to guide agencies' efforts. Further actions to improve CIP include developing a national CIP strategy and improving analysis and warning capabilities and information sharing on threats and vulnerabilities.**
Source: Report: http://www.gao.gov/cgi−bin/getrpt?GAO−03−121 Highlights: http://www.gao.gov/pas/2003/d03121high.pdf

25. *January 30, Federal Computer Week* — **INS launches student tracker.** The Immigration and Naturalization Service today will launch its Student and Exchange Visitor Information System (SEVIS), which will compile an extensive database of information about foreign students, teachers and exchange visitors. **Thursday January 30th is the deadline by which universities and other organizations with foreign students must begin reporting data on new foreign students, faculty and staff. During the summer, they must compile and report data on current foreign visitors and finish by Aug. 1. Then they must update the data regularly. INS wants to collect such information as students' addresses, visa classification, country of citizenship and credit hours completed.** Current immigration law already requires schools to collect much of the information, said INS spokesman Christopher Bentley. However, they were not required to regularly report it to INS. Congress ordered the SEVIS system in 1996, but the 2001 terrorist attacks gave the program new urgency, and the compliance deadline was moved from 2005 to 2003. Schools that don't take part in SEVIS will no longer be able to accept foreign students or issue immigration documents, Bentley added. About 600,000 foreign visitors in the United States will be subject to the reporting requirements, he said. **Meanwhile, INS is still working to certify schools that have applied to participate, he said. INS has approved more than 3,000 schools, with about 2,300 still waiting.**
Source: http://www.fcw.com/fcw/articles/2003/0127/web−sevis−01−30−03 .asp

26. *January 30, Washington Post* — **Bush to seek funds for fighting 'Dirty Bombs'.** President Bush will ask Congress next week for millions of additional dollars to prevent radiological "dirty bomb" attacks by terrorists. Energy Department figures released yesterday call for a 30 percent jump in overall spending on initiatives for preventing the spread of weapons of mass

destruction −− a threat that Bush described in Tuesday's State of the Union address as the "gravest danger facing America and the world." **Parts of the proposed budget include plans to more than double the current $16.3 million in spending on securing radiological material that could be used in making a "dirty bomb," a crude device that uses conventional explosives to spread radioactive material.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A63394−2003Jan 29.html

27. *January 30, Washington Post* — **Agency to concentrate intelligence analysis.** President Bush's decision to create a new threat assessment center could dramatically remake the way the U.S. government analyzes and responds to terrorist threats, but it is also aimed at heading off even more drastic changes sought by some lawmakers, administration officials and intelligence experts said on wednesday. **Under the plan, the threat center will provide analysis of intelligence information gathered by the CIA, FBI, Pentagon and Department of Homeland Security and will be staffed by top counterterrorism officials from each of those agencies. The center will be primarily responsible for relaying threat analysis to the president and for compiling the "daily threat matrix" that serves as the fulcrum for most intelligence decisions at the White House, officials said. For the first time, one group will have the task of analyzing data gathered by U.S. agents in this country and overseas. The analysts will pore over transcripts of tape−recorded conversations, assess tips from FBI informants, scrutinize satellite photos of overseas weapons labs, study terrorism updates from foreign security agencies and read the confessions of al Qaeda prisoners.** The plan is a clear response from Bush to rising demands in Congress and the recommendations of various terrorism panels for improved information−sharing between federal agencies. "The president believes that with the creation of this center he will be able to bring together all sources of intelligence in the United States, to deal with connecting the dots, if you will, on the threats that face us here on the homeland, as well as abroad," one senior government official said.
Source: http://www.washingtonpost.com/wp−dyn/articles/A63192−2003Jan 29.html

28. *January 30, Washington Post* — **U.S. consulate in Mexico shut in visa probe.** The U.S. government on wednesday abruptly shut its consulate in Nuevo Laredo, Mexico, announcing an investigation into whether U.S. personnel there were selling visas. **The unusual step of halting operations at one of the busiest U.S. consulates was taken because the allegations of the sale of passage into the United States were felt to be particularly serious at a time when the Bush administration is trying to tighten border controls in the wake of the Sept. 11, 2001, terrorist attacks.** "We have begun an aggressive investigation into allegations of visa fraud," said Tony Garza, the U.S. ambassador here. "We will not tolerate fraudulent activity in the processing of documents for entry into the U.S. from Mexico." Mexican police officials said they learned in November that Mexican citizens who had visited the Nuevo Laredo consulate were approached with illegal offers to buy visas. The Mexican authorities passed on that information to U.S. officials, they said. The Justice Department has not yet charged or arrested anyone in the case. **Tourist visas and "laser visas" for border residents −− a new scannable border−crossing card that is supposed to be tamper−proof −− are the main types of visas that officials believe may have been illegally sold. The visas, which cost $100 at the consulate, can fetch thousands of dollars on the black market.** A multimillion−dollar counterfeit document industry has long existed on the Mexican side of the border. But U.S. officials have been more vigorously scrutinizing documents and allegations of illegal entry since the Sept. 11 terrorist attacks.

Source: http://www.washingtonpost.com/wp−dyn/articles/A63810−2003Jan 29.html

29. *January 30, Associated Press* — **Feds with fake IDs get past border guards.** Government investigators armed with fake IDs and fictitious names had no trouble getting past U.S. border guards who didn't even bother to check the false papers in some cases, the General Accounting Office says. **Testing border security at the request of two U.S. senators, the investigative arm of Congress found the Immigration and Naturalization Service and U.S. Customs Service never questioned the authenticity of the counterfeit documents the investigators carried.** "Our agents encountered no difficulty entering the country using them," GAO official Robert Cramer said in prepared congressional testimony. Cramer, managing director of the GAO's Office of Special Investigations, said the investigators created fictitious driver's licenses and birth certificates using off−the−shelf computer graphic software available to the public, and got credit cards in the fictitious names. Senate Finance Committee Chairman Charles Grassley, (R−IA), and the panel's ranking Democrat, Max Baucus of Montana, had requested the undercover operation. **A government source said the lax security was at Miami International Airport, which Homeland Security Director Tom Ridge is to tour Thursday; and border crossings at the San Isidro section of San Diego, across from Tijuana, Mexico; Peace Arch Park in Blaine, Wash., south of Vancouver, British Columbia; and Port Angeles, Wash., where ferry boats dock from Port Victoria, British Columbia. The flight to Miami was from Jamaica, said the source, who spoke on condition of anonymity. The ferry boat crossing at Port Angeles, Wash., is where Ahmed Ressam, convicted of plotting a terrorist attack on Los Angeles Airport during millennium celebrations, was arrested in 1999 while trying to enter from Canada in a car full of explosives.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A509−2003Jan30 .html Report: http://www.gao.gov/cgi−bin/getrpt?GAO−03−438T

30. *January 29, Government Executive* — **House to create homeland security appropriations subpanel.** House Appropriations Chairman C.W. (Bill) Young, R−Fla., plans to announce the creation of a new Homeland Security Appropriations Subcommittee that will oversee the major functions of the Homeland Security Department created last year. **The proposal, which is still subject to approval by the full Appropriations Committee, would put all the agencies in the Homeland Security Department under one subcommittee, although the total number of subcommittees will stay at 13. "Eight subcommittees have jurisdiction over facets of the new department under the current committee structure," said Young. "Creating one subcommittee will allow us to focus our attention and resources on the unique challenges confronting the new department." Rep. Harold Rogers, R−Ky., who was supposed to chair the Transportation Appropriations Subcommittee again this year, will instead chair the new Homeland Security Appropriations Subcommittee, which will oversee two agencies with which Rogers is already familiar—the Transportation Security Agency and the Coast Guard. Both were previously under the Transportation subcommittee's jurisdiction. The proposal also creates a new Transportation and Treasury Appropriations Subcommittee, which will be chaired by Rep. Ernest Istook, R−Okla., who had chaired the Treasury−Postal Appropriations Subcommittee. The plan basically moves all non−homeland security−related functions from the current Transportation subcommittee to the new Transportation−Treasury subpanel, including the FAA, highways and highway safety, transit programs, safety, Amtrak, the National Transportation Safety Board and the Washington Metro Area Transit Authority.** Two

agencies currently overseen by the Commerce−Justice−State subcommittee—the Maritime Administration and the Federal Maritime Commission—will also move to Transportation−Treasury. A spokeswoman for the Senate Appropriations Committee had no comment on Young's proposal, and it is unclear whether the Senate panel will follow suit or when it might take up its own reorganization plan.
Source: http://www.govexec.com/dailyfed/0103/012903cd2.htm

[Return to top]

Emergency Services Sector

31. *January 22, Federal Emergency Management Agency* — **FEMA, USFA AND NFPA national study identifies service gaps in America's fire departments .** The Federal Emergency Management Agency (FEMA) and United States Fire Administration (USFA)on January 22nd announced a comprehensive study that examined the needs and response capabilities of the nation's fire service. The National Fire Protection Association (NFPA) conducted the Needs Assessment Study of the U.S. Fire Service for the USFA to establish a current understanding of problem areas to guide future planning and initiatives to enhance fire services and firefighter safety. The Needs Assessment Study of the U.S. Fire Service conducted by the NFPA found: **Many of the nation's fire departments do not have enough fire stations to achieve widely recognized response−time guidelines and lack key equipment, prevention programs, and a wide range of training. Approximately a third of all firefighters per shift are not equipped with self−contained breathing apparatus (SCBA). Most fire departments do not have the ability to handle unusually challenging incidents with local specialized resources and do not have written agreements to direct use of non−local response resources. In general, fire departments do not have enough portable radios to equip more than about half of the emergency responders on a shift and most radios lack intrinsic safety in an explosive atmosphere are and not water−resistant.** The USFA is implementing and supportive of solutions to address the findings of the assessment. **EMA and the USFA is about to complete the distribution of over $330 million to more than 5000 departments through last years Assistance to Firefighters Grant Program established by Congress and the President. Funds were targeted to firefighter operations, safety initiatives, new vehicle purchases, EMS training and equipment and fire prevention programs.** Planning for the 2003 Assistance to Firefighters Grant Program is underway.
Source: Report: http://www.usfa.fema.gov/downloads/pdf/publications/fa−240.p df
http://www.usfa.fema.gov/dhtml/media/03−014.cfm

[Return to top]

Information and Telecommunications Sector

32. *January 30, New York Times* — **In net attacks, defining the right to know.** After the Slammer worm attacked the Internet last weekend Bank of America discovered that thousands of its ATM's could not dispense cash. Bank officials disclosed that Slammer had created the problem only after receiving inquiries from news organizations. **To many consumer advocates, full disclosure should be the only option, especially when it comes to companies that deal with**

personal finances. In reality, few computer attacks are ever reported, and the ones that are made known tend to be those that affect thousands of computers. The **fear of publicity and a damaged reputation deters companies from reporting computer crimes to law enforcement officials**, said Roman Danyliw of the CERT Coordination Center, a federally financed information clearinghouse for computer security. In a paper presented at a cryptography conference this week, Harvard researchers Michael Smith and Stuart Schechter argued that **if an organization tells others about its security holes and the fixes it has made to them, then others have the opportunity to make the same changes and spread the word**. They claim that hackers would prefer a company that has not reported news of a break−in to one that has. In the SQL Slammer attack last weekend, system administrators were remiss about installing a security patch to the Microsoft SQL Server 2000 software, even though the patch had been available since last summer. **When neglect is the cause, it reinforces a reluctance to go public**. Schechter warns **the sharing of information can go only so far in preventing breaches. The onus is on the user to act on security advice: "People need to actually patch their systems when flaws are found. Until then, attacking systems will be as easy as figuring out which known vulnerabilities haven't been patched, then exploiting them**." Source: http://www.nytimes.com/2003/01/30/technology/circuits/30secu .html

33. *January 28, PC Magazine* — **Network attacks emerging from countries with no cybercrime laws.** Gaps in national criminal laws are leaving doors wide open for cybercriminals, says a new report from technology management consulting firm McConnell International. It shows that **only 9 of 52 countries analyzed have extended any criminal laws to cyberspace**. The McConnell report focuses on ten types of cybercrimes in four categories, including virus distribution, network−related crimes, and data theft. "The long arm of the law does not yet reach across the global Internet," says Bruce W. McConnell, the firm's president. Meanwhile, cybercriminals are reaching out from all over the globe. **Many of the most insidious viruses and network attacks of the past two years have emerged from places where no laws restrict the activities of cybercriminals**. Copies of existing and draft laws broken down by country, along with the report itself, are available at www.mcconnellinternational.com. Source: http://www.pcmag.com/article2/0,4149,850504,00.asp

34. *January 28, BBC News* — **How the Net leaves itself open to attack. Researchers at the San Diego Supercomputer Center (SDSC) in California have analyzed traffic received by one root server on October 4 last year and found that it spent most of its time dealing with unnecessary queries**. On that day **the server received more than 152 million queries and the researchers estimate that 98% of these requests were unnecessary**. Analysis of the figures showed that 70% of the requests for net addresses were duplicates − essentially different people looking for the same sites. The SDSC scientists say **all these queries could easily be dealt with if frequently requested information were held, or cached, by net service providers**. A further 12% of the queries sent to the server were for frivolous or non−existent domains such as .elvis, .corp, and .localhost. Many of the requests sent to the server used the numeric net address of the site in question, meaning the entire request was unnecessary. "**If the system were functioning properly, it seems that a single source should need to send no more than 1,000 or so queries to a root name server in a 24−hour period**," said Duane Wessels, a researcher from the Cooperative Association for Internet Data Analysis at the SDSC. "Yet we see millions of broken queries from certain sources," he said. The researchers believe that **many of the requests are due to badly configured networks that allow computers to**

make queries but do not let the reply return to the requesting computer. As a result many computers continue to request addresses fruitlessly over and over again. The report and advice comes as the net recovers from the damage wrought by the Slammer worm that exploited holes in Microsoft software.
Source: http://news.bbc.co.uk/2/hi/technology/2699071.stm

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 www.securityfocus.com

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **PE_FUNLOVE.4099** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 1434 (ms−sql−m), 1433 (ms−sql−s), 53 (domain), 80 (http), 445 (microsoft−ds), 4662 (???), 21 (ftp), 135 (???), 443 (https) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

35. *January 30, Boston Globe* — **Shoebomber's low−tech style is seen as future of terrorism.** Like shoebomber Richard Reid, operatives in the network of underground sleeper cells have not received the kind of sophisticated training that characterized the Sept. 11 hijackers. They support each other through a clandestine network that can provide credit cards, fake identity documents, money for travel expenses, and safe houses. And like Reid, they are expected to find ways to strike at the declared enemies of al Qaeda and its affiliated terror groups: the United States, its allies, their military forces, and their citizens. **"Think of the Sept. 11 terrorists as the A−team terrorist weapons and a Richard Reid as a kind of B−team," Walter Purdy, director of the Terrorism Research Center in Virginia, said. "What makes a person like Richard Reid so valuable is that you don't have to spend a lot of time training him." Reid received rudimentary weapons instruction in Afghan camps. Others like him after Sept. 11 might have received on−the−fly training in Europe or Southeast Asia, according to antiterrorism specialists. "A group like al Qaeda can send a whole group of people like this across the world," Purdy said.** Even if they fail, as Reid did, the attempted attacks can siphon law enforcement resources and force costly changes in air travel security practices. **Authorities still don't know who made Reid's shoe bomb, and how close**

he was to al Qaeda's brain trust. But to investigators on both sides of the Atlantic, it's becoming increasingly apparent that many future terrorist attacks will be mounted by people like him.
Source: http://www.boston.com/dailyglobe2/030/metro/Shoebomber_s_low_tech_style_is_seen_as_future_of_terrorism+.shtml

36. *January 30, CNN* — **Arrests raise concern over tech spies.** The case of a Chinese businessman charged with illegally shipping missile guidance technology to China's military has intensified concerns about foreign espionage in Silicon Valley. **Qing Chang Jiang, who was arraigned last week, is at least the fourth Chinese native indicted since October on charges involving the shipment of equipment or trade secrets to China from the nerve center of the U.S. technology industry. Prosecutors worry Jiang may have been illegally exporting technology to China since 1998, when he bought one of the world's fastest computers from a federal weapons lab.** Although it never left the United States, the sale was a major embarrassment for Sandia National Laboratories. Officials acknowledged it was an act of "enormous stupidity." **A spokesman for the Chinese Consulate in San Francisco said his government has no relationship with Jiang, who also has gone by Frank Jiang, Frank White and Korber Jiang. "It's his personal behavior," Lei Hong said. "I'm not aware of the details, but the Chinese government does not support that type of behavior."** Jiang first raised eyebrows in 1998 when he managed to buy the Intel Paragon XPS computer. A $10 million machine when purchased five years earlier, the Paragon had been used for classified projects. After scientists deemed it obsolete, the Paragon was disassembled. The drives and disks that had been used for classified computing were removed. The remaining two−thirds was offered on the open market and purchased by EHI Group USA for $30,800 in October 1998. Jiang soon contacted Intel Corp. and asked how to replace the missing parts. **Concerned that the machine would be used in China, Intel notified the laboratory, prompting a federal investigation. Inspectors later found the Paragon, still wrapped in plastic in Jiang's warehouse, and bought it back for $88,888.** "If it had been successfully reassembled, made operational and combined with appropriate computer software, such a computer could have been useful for nuclear weapon applications," C. Paul Robinson, Sandia's director at the time, told Congress.
Source: http://www.cnn.com/2003/TECH/biztech/01/30/silicon.spies.ap/ index.html

37. *January 30, Reuters* — **Iraq UN envoy warns of attacks on U.S. interests. Iraq's U.N. ambassador, Mohammed Aldouri, warned on Wednesday that Muslims around the world would attack American facilities if the United States invaded his country.** He told Reuters in an interview **he did not believe such outbursts, from Indonesia to the Middle East, would be coordinated but would form a spontaneous response to an invasion.** "Certainly United States interests will be endangered in the Arab world and the Muslim world. I am certain of that," Aldouri said. "They cannot accept that a whole country will be attacked."
Source:
http://story.news.yahoo.com/news?tmpl=story20030130/ts_nm/iraq_un_response_dc_4ont>

[Return to top]

NIPC Products &Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web−site (http://www.nipc.gov), one can quickly access any of the following NIPC products:

NIPC Advisories − Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

NIPC Alerts − Alerts address major threat or incident information addressing imminent or in−progress attacks targeting specific national networks or critical infrastructures.

NIPC Information Bulletins − Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

NIPC CyberNotes − CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure−related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:	Melissa Conaty (202−324−0354 or mconaty@fbi.gov) Kerry J. Butterfield (202−324−1131 or kbutterf@mitre.org)
Distribution Information	NIPC Watch and Warning Unit (202−323−3204 or nipc.watch@fbi.gov)

NIPC Disclaimer